Project Documentation

# Project Title: AI-Based XSS Payload Recommender

The AI-Based XSS Payload Recommender is a security-focused project that aims to assist penetration testers   
and security researchers in identifying effective Cross-Site Scripting (XSS) payloads based on the context of   
a web application's input. The recommender system uses a machine learning approach (or optionally, OpenAI APIs)   
to generate or suggest suitable payloads for different scenarios, enhancing the productivity of ethical hackers.

## Project Description

This project provides a user-friendly interface where users can input test cases or scenarios, and the AI   
component processes the context to generate relevant XSS payloads. It includes the following components:  
- A front-end interface built with React  
- A backend server using Flask (Python)  
- An AI/ML module to recommend XSS payloads based on prompts  
- Integration with XSS payload databases

## Features

- Real-time payload recommendation based on user input.  
- Clean UI interface with seamless UX.  
- Secure Flask backend API for interaction with AI model.  
- Logging functionality to keep track of previous queries and payloads.

## Technologies Used

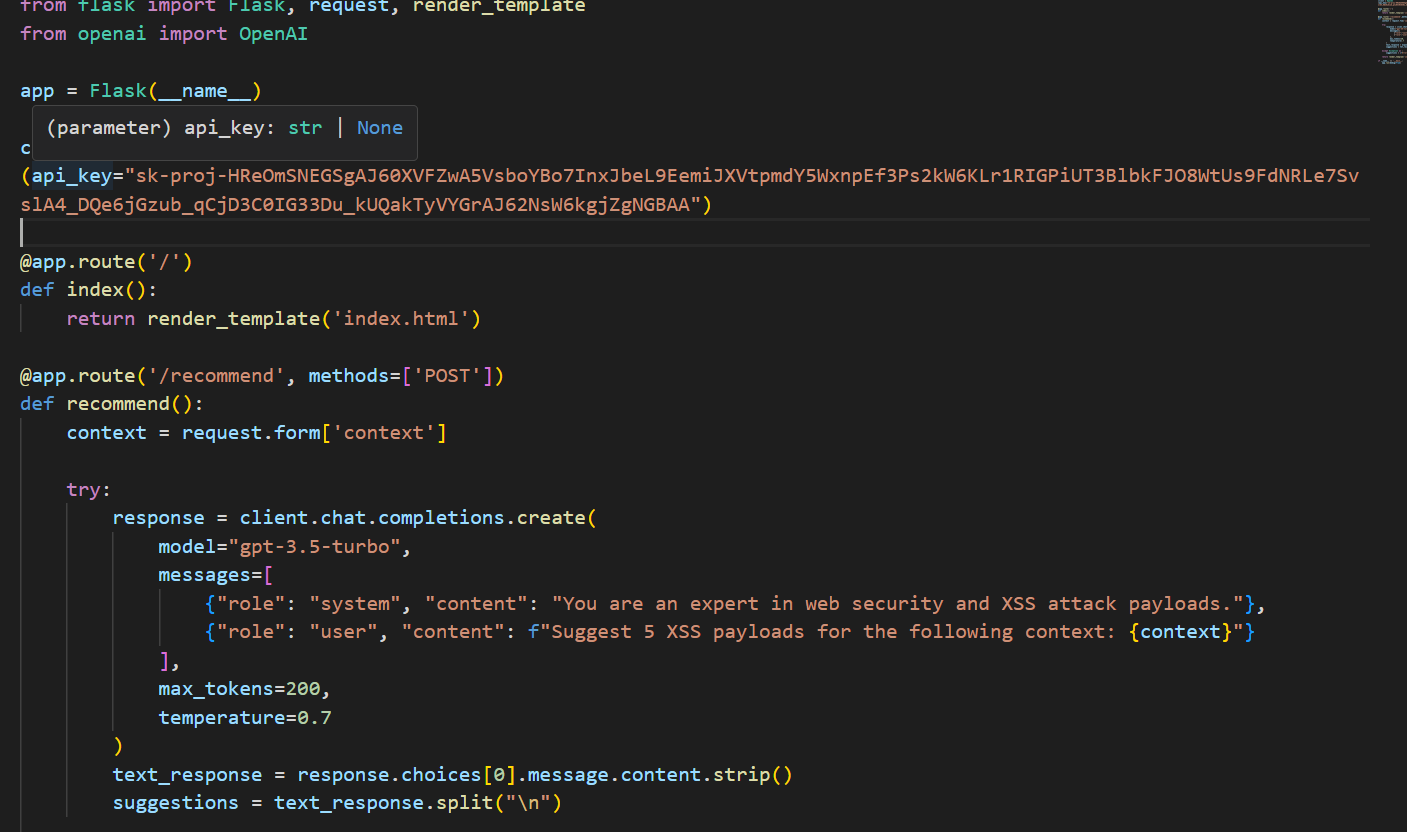
- Frontend: ReactJS, HTML/CSS  
- Backend: Python, Flask  
- AI: OpenAI API / Machine Learning Model (custom-trained)

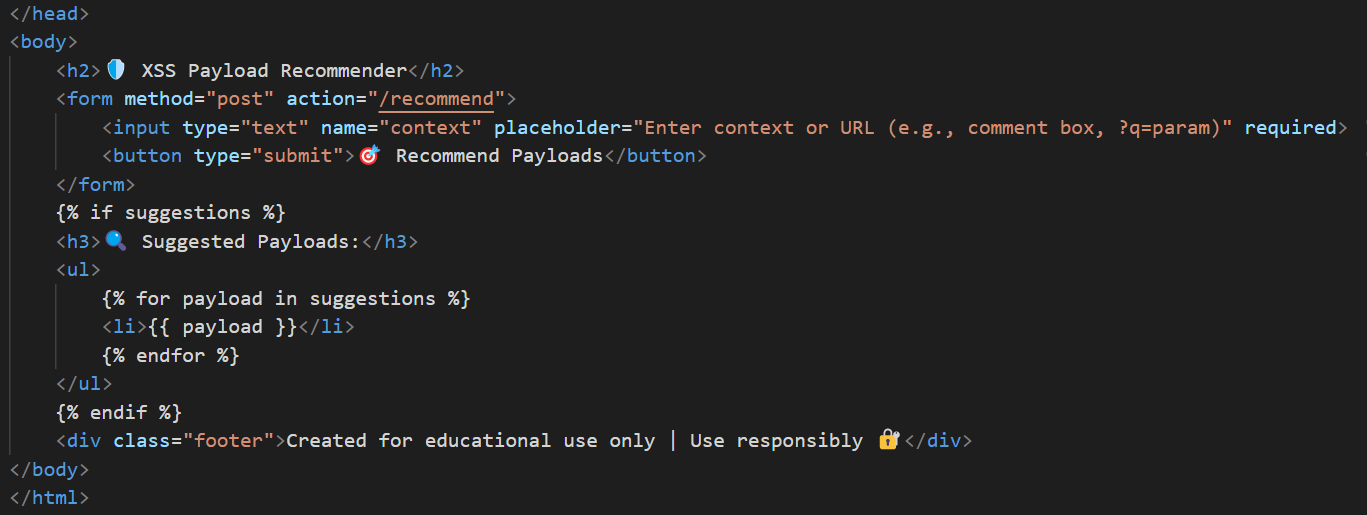
## How It Works

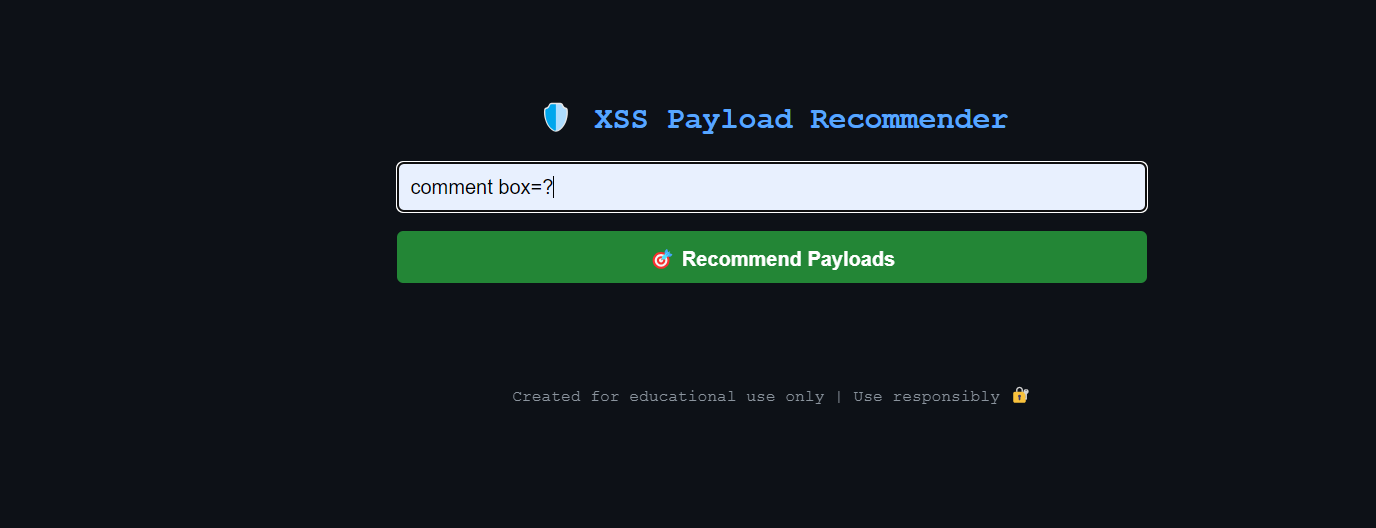
1. User enters a context or HTML/JS-based scenario.  
2. Flask backend processes the input.  
3. AI model returns a relevant XSS payload.  
4. Payload is shown in the UI with copy and log options.

## Conclusion

The AI-Based XSS Payload Recommender is a valuable tool in the arsenal of ethical hackers and penetration   
testers, enabling faster, more targeted security testing and automation of basic payload generation.







Submitted by: Giriraj Mangalvedhe